REMARKS/ARGUMENTS

Claims 1-28 and 33-35 are pending in the present application. Claims 1, 4, 7, 10, 13, 17, 21 and 25 are independent claims. Claim 35 is added by this Amendment.

Reply to Examiner's Response to Arguments

Since the Examiner has maintained the prior rejections and has provided arguments in support of this position, Applicant will address the Examiner's response first.

1. Clarification requested regarding an apparent inconsistent statement made by the Examiner

In the 12/15/2008 Final Rejection, the Examiner stated that "Applicant notes that Alden fails to disclose 'sequential code encryption'. However, Citta was used for this limitation, as also acknowledged by Applicant" (e.g., see Page 3 of the 12/15/2008 Final Rejection). The Examiner also stated that "neither Alden nor Citta particularly discloses using a sequential code for which a unique key is derived for encrypting the data" (e.g. Page 4 of the 12/15/2008 Final Rejection. The Examiner also stated that "Alden et al does not disclose that the encryption is based on sequential code encryption" (e.g., see Page 8 of the 12/15/2008 Final Rejection).

In the subsequent Advisory Action of 3/23/2009, the Examiner appears to have changed positions entirely on this matter, and now asserts the following:

> The examiner respectfully disagrees and submit that Alden et al discloses that a first transport frame comprising a first portion and a second portion of **said first sequential code** ...
>
> (e.g., see the 3/23/2009 Advisory Action, Emphasis added)

Accordingly, it is Applicant's understanding that the Examiner is now arguing that Alden does, in fact, disclose the claimed "sequential code", as the Examiner appears to argue that

Alden's transport frame includes first and second portions of the sequential code as claimed. Applicant respectfully requests a clarification on this issue in a subsequent Office Action.

2. Remarks related to the Examiner's arguments related to Alden in the Advisory Action

Assuming the Examiner has changed positions regarding the teachings of Alden as discussed in the preceding section, Applicant still does not believe Alden in combination with Citta and/or Barnett render the claimed subject matter as obvious.

In the 3/23/2009 Advisory Action, the Examiner cites to Figure 7 and Column 10, lines 24-45 of Citta for allegedly disclosing "encapsulating said first encrypted data frame in a first transport frame, said first transport frame comprising a first portion and a second portion of said first sequential code" as recited in independent claim 1. As an initial matter, Applicant notes that Column 10, lines 24-45 correspond to a description of Figure 8 of Alden, not Figure 7. The cited portion of Alden reads as follows:

> The field 156 contains an offset into the frame at which key exchange data as is stored, for example within the string buffer field 163. The key exchange data for example includes key exchange material to be used for encryption/decryption over the life of the tunnel connection and any validity times associated with that key exchange material. The key exchange data, as well as the field 158, further includes information regarding any shared set of cryptographic transforms to be applied to subsequent data and any other connection-specific parameters, such as strength and type of cipher to be used, any compression of the data to be used, etc. The field 160 contains flags, for example indicating other information about the frame. The client data field 162 contains data used by the pseudo network adapters in the tunnel end points to configure the local routing tables so that packets for nodes in the virtual private network are sent through the pseudo network adapters. The string buffer includes key exchange material. The string buffer is for example encrypted using a public encryption key of the receiving tunnel end point, in the this case the initiator of the tunnel connection.
>
> *(e.g., see Col. 10, lines 24-44 of Alden, Emphasis added)*

To put the above-section of Alden in perspective, Alden teaches sending key exchange/authentication requests (e.g., see step 90 of FIG. 5 of Alden) and receiving key exchange/authentication responses (e.g., see step 92 of FIG. 5 of Alden). FIG. 7 of Alden shows

how the request of step 90 is configured, and FIG. 8 of Alden shows how the response of step 92 is configured. In the message exchange of steps 90 and 92, key exchange material is negotiated in order to establish a key to be used during a future communication session for encryption/decryption.

The emphasized-portions shown above with respect to FIG. 8 of Alden show that the key exchange material is contained in the string buffer field 163. The string buffer field 163 is encrypted with a public encryption key, not a key related to the key exchange information itself. Alden cannot use the session key currently being negotiated for the encryption because the key has not yet been negotiated. If this were even possible, conducting the negotiation would make no sense, because Alden would simply start encrypting/decrypting data packets and would not bother conducting the negotiation in the first place.

Turning to claim 1, Applicant has claimed "encrypting a first data frame based on a ... first sequential code", and then "encapsulating said first encrypted data frame in a first transport frame ... comprising ... said first sequential code". By contrast, Alden simply teaches encrypting and decrypting a key-portion during a key-negotiation with a public key.

If the Examiner reads the claimed "sequential code" upon the public key used to encrypt the packets of steps 90 and/or 92 in FIG. 5 of Alden, Applicant notes that the public key is not actually included in either packet; rather, the encrypted portion correspond to the key currently being negotiated, not the public key. Thus, under this interpretation, Alden would fail to disclose or suggest claimed "encrypting a first data frame based on a ... first sequential code", and then "encapsulating said first encrypted data frame in a first transport frame ... comprising ... said first sequential code" a recited in claim 1 (Emphasis added).

Alternatively, if the Examiner reads the claimed "sequential code" upon the key exchange material included in the string buffers of the packets of steps 90 and/or 92 in FIG. 5 of Alden,

Applicant notes that the key exchange material is not actually used for encrypting either packet; rather, the public key is used to encrypt the packet, and the devices have to wait until after the key-negotiation to use the key exchange material for actual encryption or decryption. Thus, under this interpretation, Alden would fail to disclose or suggest claimed "encrypting a first data frame based on a … first sequential code", and then "encapsulating said first encrypted data frame in a first transport frame … comprising … said first sequential code" a recited in claim 1 (Emphasis added).

Accordingly, under either interpretation, Alden's disclosure fails to cure the deficiencies of Citta and/or Barnett. The deficiencies of both of these references have been discussed in detail in prior responses filed by the Applicant, and these arguments will not be regurgitated herein for the sake of brevity.

3. The Examiner's arguments related to the 35 U.S.C. § 103(a) rejection based on Barnett does not address claim language argued by Applicant as distinguishing over each applied reference.

The Examiner and Applicant are in agreement in that Alden (6,101,543) and Citta (4,771,458) do not disclose "using a sequential code for which a unique key is derived for encrypting the data" (e.g., see Page 4 of the 12/15/2008 Final Rejection). In the After-Final response filed by Applicant on 2/13/2009, Applicant argued that even assuming that Barnett discloses this particular feature, Barnett does not disclose or suggest including its character string in packets that are encrypted based on its character string, and as such cannot disclose "first transport frame comprising a first portion and a second portion of said first sequential code" as recited in independent claim 1, for example.

The Examiner's response to this argument as articulated in the 3/23/2009 Advisory Action was not to allege that Barnett actually discloses the argued limitation, but that Alden discloses the feature. Alden's alleged teachings regarding this limitation have been addressed in a preceding section.

Because the Examiner has not indicated that Barnett discloses "encapsulating said first encrypted data frame" but rather cites to Alden for this limitation, an indication that Barnett does not disclose the "encapsulating" limitation is respectfully requested from the Examiner.

4. The Examiner's comments in the 12/15/2008 Final Rejection do not address Applicant's arguments regarding the combinability of Kluttz with Alden and Citta

Applicant directs the Examiner to pages 17-19 of the 9/25/2008 Amendment. In this section, Applicant discusses Alden and Citta in detail, and demonstrates how Alden and Citta are each directed to ***transport***-layer encryption.

Applicant goes on to describe how Kluttz, on the other hand, is directed to encrypting a stored file or document (e.g., see Page 20 of the 9/25/2008 Amendment). Referring to Figures 3 and 4 of Kluttz, Kluttz teaches partitioning a document into multiple portions, and applying a different level of encryption to each portion. Portions associated with "higher" level encryption are encrypted with a higher-level specific encryption key, as well as any "lower" level encryption keys. Thus, more confidential material is protected by both the higher level encryption key as well as all lower level encryption keys. As will be appreciated by one of ordinary skill in the art, the encryption of Kluttz is directed to a file storage protocol executed at the application layer, and not at a transport layer (as in Alden and Citta).

Even assuming for the sake of argument that one of ordinary skill in the art could find some motivation to combine Alden, Citta and Kluttz, the alleged combination would not result in

the claimed invention. The methodologies associated with encryption of file storage documents, such as MS Word documents, MS Excel documents, etc., cannot simply be imported into the transport layer for encrypting TCP/IP packets. As will now be described in detail, there are fundamental differences between encryption performed at the file storage layer, or "application layer", and encryption performed at the TCP/IP layer, or "transport layer".

In Alden, the pseudo network adapter 259 is essentially "dumb". In other words, the pseudo network adapter 259 does not have any special knowledge regarding any particular packet that is encrypted/encapsulated, but rather simply encrypts/encapsulates any received packets. As is known in the art, in preparing a file document for transmission at the transport layer, the file document is broken up into payload-portions in a plurality of packets, such as TCP/IP packets, for transmission. The pseudo network adapter 259 does not evaluate the "content" of any packets, nor does the pseudo network adapter 259 evaluate or even consider the "document" from which individual packets were generated. Such actions simply are not performed at the transport layer.

Likewise, in Citta, the address of a transport-layer packet is used to determine what type of content is being received at the subscriber terminal (e.g., HBO, Showtime, etc.), and the address keys are used to decrypt that content at the subscriber terminal. The subscriber is not aware of what the content is that is being sent, but simply attempts to decode based on its personal address key, which is associated with the subscriber's permissions. If the packet cannot be decoded it is simply discarded.

Accordingly, Kluttz's method of partitioning a storage file document into different portions associated with different levels of encryptions makes no sense at the transport layer, nor is there any comparable transport layer operation that could be achieved based on the teachings of Alden and/or what is known in the art. In other words, how could a document be partitioned

when the pseudo network adapter 259 of Alden, or the subscriber in Citta, only has knowledge of an individual packet with no knowledge of that packet's association with any particular document? How could the pseudo network adapter 259 in Alden, or the subscriber in Citta, associate that packet with a corresponding portion of a document that is associated with a given level of security/encryption? Many more questions could be raised regarding this alleged "obvious" implementation or combination.

Instead of combining the references in the manner alleged by the Examiner, Applicant respectfully submits that a much more likely combination of Alden, Citta and Kluttz would simply be to (i) encrypt a file storage document at the application layer as indicated by Figure 2 of Kluttz and (ii) if it is determined to send the file storage document to another entity, to break up the file storage document into individual packets as is known in the art and process the individual packets through the pseudo network adapter 259 as described by Alden. At the receiving end, a subscriber would receive the packet, as in Citta, and attempt to decode/decrypt the packet based on its address key. In other words, because Alden or Citta and Kluttz deal with encryption at different layers, their processes would be applied separately, and not meshed together in the manner suggested by the Examiner. Applicant notes that the claims would not read upon Kluttz, Citta and Alden combined in this manner.

5. Applicant respectfully requests a clarification from the Examiner regarding the last sentence on Page 4 of the 12/15/2008 Final Rejection

The Examiner states "[t]herefore, given the limitation 'sequential code' its broadest interpretation (MPEP 2111), the following references are used for the teaching of 'sequential code'" (e.g., see Page 4 of the 12/15/2008 Final Rejection). The Examiner goes on to describe

portions of the disclosure of Perlman, Barnett and Kluttz (e.g., see Page 5 of the 12/15/2008 Final Rejection).

Regarding Barnett, Applicant at least understands how the Examiner is attempting to read "sequential code". However, Applicant is less sure regarding how this term is intended to be read regarding Perlman and/or Kluttz, or how the reading of "sequential code" upon these references affects the arguments of the Examiner. For example, while Applicant cannot be sure, it appears the Examiner reads "sequential code" upon Perlman's keys 32 and Kluttz's encryption keys 72. However, as the Examiner has not actually rejected the claims based on Perlman or Kluttz in the manner implied in this section in the Response to Arguments section of the 12/15/2008, Applicant will refrain from further comment until the Examiner reevaluates Applicant's arguments presented herein.

Further, even if Kluttz and/or Perlman were to include some teachings upon which "sequential code" could read, the *Graham v. John Deere Co.*, 383 U.S. 1 (1966) factors related to whether it would be obvious to combine these particular portions with Alden and Citta have not been addressed by the Examiner. Also, Applicant does not claim a "sequential code" in a vacuum, but also claims "encapsulating said first encrypted data frame in a first transport frame, said *first transport frame comprising a first portion and a second portion of said first sequential code*" as recited in independent claim 1, for example (emphasis added).

SUMMARY

Since the Examiner has maintained his rejection of claims 1-28 and 33-34 under 35 U.S.C. § 102 and 103 as noted above, Applicant once again traverses these rejections. Applicant expressly maintains the reasons from the prior responses to clearly indicate on the record that Applicant has not conceded any of the previous positions relative to the maintained rejections. For brevity, Applicant expressly incorporates the prior arguments presented in the September 25, 2008 response without a literal rendition of those arguments in this response.

For at least the foregoing reasons and the reasons set forth in Applicant's response of September 25, 2008, it is respectfully submitted that claims 1, 4, 7, 10, 13, 17, 21 and 25 are distinguishable over the applied art. The remaining dependent claims are allowable at least by virtue of their dependency on the above-identified independent claims. See MPEP § 2143.01. Moreover, these claims recite additional subject matter, which is not suggested by the documents taken either alone or in combination.

For example, claim 35 recites "wherein the first and second data frames carry data associated with a push-to-talk (PTT) or PTX communication session". In the Advisory Action of 3/23/2009, the Examiner reads the claimed data frames upon the packets transmitted in steps 90 and 92 of Figure 5 of Alden. However, these steps are conducted to obtain a key that is useable for encrypting a future communication session. The request/response of steps 90/92 does not carry data of any kind, other than the key being negotiated. Accordingly, these packets do not carry data associated with a PTT or PTX communication session.

CONCLUSION

In view of the foregoing amendments and remarks, it is respectfully submitted that the application is in condition for allowance. If the Examiner believes that any additional changes would place the application in better condition for allowance, the Examiner is invited to contact the undersigned attorney, at the telephone number listed below.

Deposit Account Authorization

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: 2009-04-15

By: _____
Gerald P. Joyce, III
Reg. No. 37,648

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502

Attachment(s): None